PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07C 9/00 — A1

(11) Numéro de publication internationale: **WO 99/35617**

(43) Date de publication internationale: 15 juillet 1999 (15.07.99)

(21) Numéro de la demande internationale: PCT/FR99/00023

(22) Date de dépôt international: 8 janvier 1999 (08.01.99)

(30) Données relatives à la priorité:
98/00125 8 janvier 1998 (08.01.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: LA POSTE [FR/FR]; 4, quai du Point du Jour, F–92777 Boulogne Billancourt Cedex (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: CLERC, Fabrice [FR/FR]; 33, avenue Robert Schuman, F–14000 Caen (FR). GIRAULT, Marc [FR/FR]; 9, rue Bernard Vanier, F–14000 Caen (FR).

(74) Mandataire: FRECHEDE, Michel; Cabinet Plasseraud, 84, rue d'Amsterdam, F–75440 Paris Cedex 09 (FR).

(81) Etats désignés: JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD AND SYSTEM FOR CONTROLLING ACCESS TO A RESOURCE LIMITED TO CERTAIN TIME FRAMES

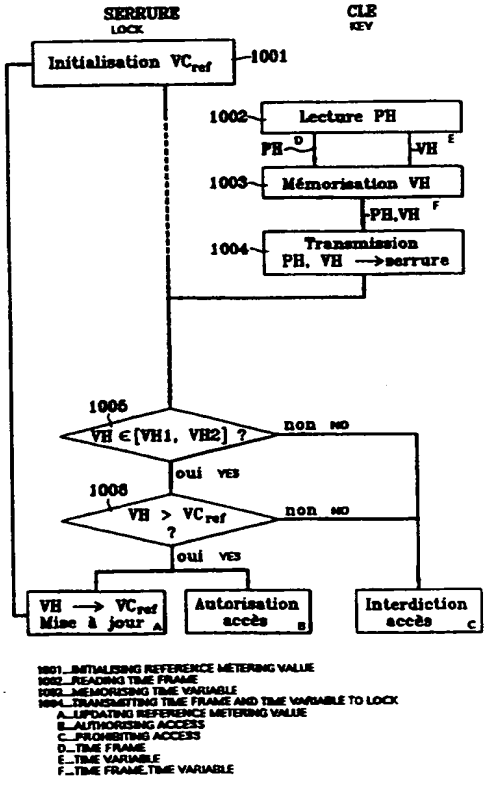
(54) Titre: PROCEDE ET SYSTEME DE CONTROLE D'ACCES A UNE RESSOURCE LIMITE A CERTAINES PLAGES HORAIRES

(57) Abstract

The invention concerns a method for controlling the access of an electronic key to an electronic lock inside a predetermined time frame which consists in; initialising the lock with a reference metering value; then, at each attempt for accessing the lock with the key: reading in the key a previously stored time frame; storing a current time value delivered by the real time clock; transmitting from the key to the lock the time frame and the current time value; and, in the lock: verifying the coherence of the current time value with the time frame; in case of coherence, authorising access, and updating the reference metering value, on the basis of the current time value transmitted; otherwise, prohibiting the key from accessing the lock.

(57) Abrégé

Pour contrôler l'accès d'une clé électronique à une serrure électronique, à l'intérieur d'une plage horaire prédéterminée: on initialise la serrure par une valeur de comptage de référence; puis, lors de chaque tentative d'accès de la clé à la serrure: dans la clé, on lit une plage horaire préalablement mémorisée; on mémorise une valeur horaire courante délivrée par une horloge temps réel; on transmet de la clé à la serrure la plage horaire et la valeur horaire courante; et, dans la serrure: on vérifie la cohérence de la valeur horaire courante avec la plage horaire, et avec la valeur de comptage de référence; s'il y a cohérence, on autorise l'accès, et on met à jour la valeur de comptage de référence, à partir de la valeur horaire courante transmise; sinon, on interdit l'accès de la clé à la serrure.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

PROCÉDÉ ET SYSTÈME DE CONTRÔLE D'ACCÈS À UNE RESSOURCE LIMITÉ À CERTAINES PLAGES HORAIRES

La présente invention concerne un procédé et un système de contrôle d'accès à une ressource limité à certaines plages horaires.

Elle s'applique au contrôle d'accès à une ressource quelconque, ressource accédée, dont on souhaite contrôler l'utilisation, et dont on souhaite limiter l'accès à une ou plusieurs plages horaires déterminées, dites aussi plages de validité prédéterminées, que la ressource considérée soit un bâtiment, un système informatique, ou tout autre objet, tel qu'une boîte aux lettres ou un coffre de banque.

L'invention s'applique plus particulièrement au contrôle d'accès à des ressources accédées non autonomes en énergie et/ou ne disposant que d'un potentiel limité de vérification d'une plage horaire de validité, notamment les ressources ne disposant pas d'horloge temps réel.

La plage de validité peut être, soit la période proprement dite pendant laquelle il est possible d'accéder à la ressource, soit tout autre paramètre permettant de limiter dans le temps une attaque par utilisation frauduleuse de la ressource accédante.

Le principal avantage d'un moyen d'accès logique à une ressource par rapport à un moyen d'accès physique réside généralement dans la possibilité de ne permettre l'accès à la ressource qu'à l'intérieur d'une plage horaire relativement courte prédéterminée.

Dans ces conditions, si la clé électronique est perdue, volée, cédée ou dupliquée, elle ne permettra pas à son détenteur illégitime d'accéder à la ressource en dehors de la plage horaire prédéterminée. Cela suppose cependant que

la ressource accédée soit en mesure de vérifier que cette plage horaire est respectée. Cela implique généralement que la ressource accédée dispose d'une horloge temps réel.

Ainsi, le document FR-A-2 722 596 décrit un système de contrôle d'accès limités à des plages horaires autorisées et renouvelables au moyen d'un support de mémorisation portable. Ce système, fondé sur des mécanismes cryptographiques, permet de limiter la période de validité des droits d'accès à une courte durée, afin d'éviter une utilisation illégitime en cas de perte, vol, cession ou duplication illicite.

Toutefois, la solution décrite repose sur l'hypothèse, fortement contraignante, que la ressource accédée soit autonome en énergie, pour maintenir une horloge temps réel lui permettant de vérifier la validité de la plage horaire dans laquelle a lieu la tentative d'accès par la ressource accédante.

La présente invention a pour but de remédier aux inconvénients précités en permettant à la ressource accédée de vérifier la plage de validité sans pour autant disposer d'une horloge temps réel.

Dans ce but, la présente invention propose un procédé de contrôle d'accès d'au moins une clé électronique, munie d'une horloge temps réel délivrant une valeur horaire courante, à au moins une serrure électronique, à l'intérieur d'une plage horaire prédéterminée, remarquable en ce que :

(a) on initialise la serrure électronique par une valeur de comptage de référence ;

puis, lors de chaque tentative d'accès de la clé électronique à une serrure électronique :

dans la clé électronique :

(b) on lit une plage horaire prédéterminée, préalablement mémorisée dans la clé électronique ;

(c) on mémorise une valeur horaire courante délivrée par l'horloge temps réel ;

(d) on transmet de la clé électronique à la serrure électronique la plage horaire et la valeur horaire courante, et

dans la serrure électronique :

(e) on vérifie que la valeur horaire courante transmise est à l'intérieur de la plage horaire prédéterminée, et qu'elle est postérieure à la valeur de comptage de référence mémorisée dans la serrure ;

(f) si les vérifications effectuées à l'étape (e) sont satisfaites, on autorise l'accès, et on met à jour la valeur de comptage de référence, à partir de la valeur horaire courante transmise ;

(g) si la valeur horaire courante transmise est à l'extérieur de la plage horaire prédéterminée, ou si elle est antérieure à la valeur de comptage de référence mémorisée dans la serrure, on interdit l'accès de cette clé à cette serrure.

Dans un mode de réalisation qui procure une sécurité accrue, on effectue les étapes supplémentaires ci-après.

Dans la clé électronique :

(b1) à l'étape (b), on lit, en plus de la plage horaire, ou en lieu et place de la plage horaire, une signature électronique de la plage horaire, préalablement calculée et mémorisée dans la clé électronique ;

(d1) à l'étape (d), on transmet de la clé électronique à la serrure électronique, en plus de la plage horaire, ou en lieu et place de la plage horaire et de la valeur horaire courante, la signature et la valeur horaire courante, et

dans la serrure électronique :

(e1) avant l'étape (e), on vérifie la signature transmise, à partir d'une clé de vérification spécifique ;

(f1) à l'étape (f), on n'autorise l'accès, et on ne met à jour la valeur de comptage de référence, à partir de la valeur horaire courante transmise, que si les vérifications effectuées aux étapes (e1) et (e) sont satisfaites ;

(g1) à l'étape (g), on interdit l'accès de cette clé à cette serrure si la valeur horaire courante transmise est à l'extérieur de la plage horaire, ou si elle est antérieure à la valeur de comptage de référence mémorisée dans la serrure, ou si la vérification effectuée à l'étape (e1) n'est pas satisfaite.

En variante, l'ordre d'exécution des étapes (e1) et (e) peut être interverti.

La clé de vérification spécifique utilisée à l'étape (e1) peut être une clé publique ou secrète.

La plage horaire précitée peut comprendre plusieurs plages horaires disjointes.

Dans un mode particulier de réalisation, la plage horaire est un intervalle comportant deux bornes exprimées chacune comme une date en jour, mois, année et un horaire en heures, minutes, secondes.

La présente invention propose également un système de contrôle d'accès électronique, à l'intérieur d'une plage horaire prédéterminée, comportant au moins une serrure électronique et au moins une clé électronique, remarquable en ce que la clé comprend

- une horloge temps réel délivrant une valeur horaire courante, et

- un module de transmission à la serrure d'une plage horaire prédéterminée, et en ce que la serrure comprend
- un module de mémorisation accessible en lecture et en écriture,
- un module de comptage, ce module de comptage étant mis à jour à partir de la valeur horaire courante à chaque tentative d'accès réussie, et
- un module de comparaison de la valeur horaire courante à la plage horaire prédéterminée et à la valeur mémorisée dans le module de comptage.

Dans un mode de réalisation qui procure une sécurité accrue, le module de transmission à la serrure d'une plage horaire prédéterminée s'accompagne d'un module de transmission à la serrure d'une signature électronique de la plage horaire, et la serrure comprend en outre un module de vérification de la signature électronique transmise par la clé.

Dans un mode particulier de réalisation, le module de mémorisation comprend une mémoire non volatile reprogrammable électriquement.

Dans un mode particulier de réalisation, la clé électronique communique avec la serrure électronique à l'aide d'un module de transmission sans contact, par induction électromagnétique.

Ce module de transmission sans contact peut comprendre un premier bobinage électromagnétique prévu dans la clé et un second bobinage électromagnétique prévu dans la serrure.

Ces deux bobinages peuvent être concentriques.

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description

détaillée qui suit d'un mode particulier de réalisation, donné à titre d'exemple non limitatif.

La présente invention se réfère aux dessins annexés, dans lesquels :

- la figure 1 est un organigramme du procédé de contrôle d'accès de la présente invention, dans un mode particulier de réalisation ;
- la figure 2 est un organigramme du procédé de contrôle d'accès de la présente invention, dans un autre mode particulier de réalisation ;
- la figure 3 représente de façon schématique le système de contrôle d'accès de la présente invention, dans un mode particulier de réalisation ;
- la figure 4 représente de façon schématique le système de contrôle d'accès de la présente invention, dans un autre mode particulier de réalisation ; et
- la figure 5 représente de façon schématique le module de transmission sans contact permettant à la clé électronique de communiquer avec la serrure électronique, dans un mode particulier de réalisation.

Dans toute la suite, on considère une clé électronique utilisée pour une tentative d'accès à une serrure électronique. La clé et la serrure électroniques disposent d'une unité de calcul. La clé électronique est munie d'une horloge temps réel. Cette horloge temps réel délivre une valeur horaire courante VH, exprimée par exemple en jour, mois, année, heures, minutes, secondes. On souhaite limiter l'accès de la clé à la serrure à une plage horaire donnée PH, définie comme l'intervalle de temps compris entre deux valeurs horaires VH1 et VH2 déterminées : PH = [VH1,VH2], ou

de manière plus large comme une réunion de tels intervalles : PH = [VH1,VH2]∪[VH3,VH4]∪...∪[VHn-1,VHn].

Comme l'indique la figure 1, une première étape 1001 du procédé consiste à initialiser la serrure électronique par une valeur de comptage de référence VC_{ref}.

On considère ensuite une situation où la clé électronique tente d'accéder à la serrure électronique. Cette situation peut se traduire de diverses façons, selon la forme et la nature des supports contenant la clé et la serrure. A titre d'exemple non limitatif, si la clé comporte une partie tubulaire ou en forme de languette plate, la tentative d'accès se fait par introduction de la partie tubulaire dans une cavité tubulaire complémentaire de la serrure, ou dans une fente complémentaire, respectivement.

Un protocole de vérification du droit d'accès de cette clé à cette serrure est alors mis en œuvre successivement dans la clé et dans la serrure.

Dans la clé, comme indiqué en 1002 sur la figure 1, on lit une plage horaire prédéterminée PH, qui a été préalablement mémorisée dans la clé électronique.

Comme indiqué en 1003, lors de la tentative d'accès, on mémorise dans la clé la valeur horaire courante VH délivrée par l'horloge temps réel de la clé.

Puis on transmet, en 1004, la plage de validité ainsi que la valeur horaire courante VH à la serrure.

Les étapes suivantes de vérification ont alors lieu dans la serrure.

En 1005 et 1006, on vérifie, d'une part, la cohérence entre la valeur horaire courante transmise VH et la plage horaire prédéterminée PH, et d'autre part, la cohérence

entre VH et la valeur de comptage de référence VC_{ref} mémorisée dans la serrure.

Par exemple, dans le cas d'une plage horaire réduite à un intervalle [VH1,VH2], on vérifie que VH est postérieure à VH1 et antérieure à VH2, et que VH est postérieure à VC_{ref}.

Si l'une des vérifications effectuées aux étapes 1005 et 1006 donne lieu à une réponse négative, on interdit l'accès de cette clé à cette serrure.

Si l'ensemble de ces vérifications a été satisfait, on autorise l'accès, et on met à jour VC_{ref} en la remplaçant par exemple par la valeur horaire courante VH.

On décrit ci-après un autre mode de réalisation du procédé de l'invention, qui procure une sécurité accrue par rapport au mode de réalisation précédent.

On considère une ressource accédée non autonome en énergie et/ou ne disposant que d'un potentiel limité de vérification d'un droit d'accès.

Par « droit d'accès », on entend la signature électronique d'une plage de validité. Une signature électronique peut être obtenue à l'aide de mécanismes cryptographiques divers, tels que des mécanismes de chiffrement, ou d'authentification. Elle peut par exemple être obtenue à l'aide d'un algorithme de signature à clé secrète ou d'un algorithme de signature à clé publique.

Lorsqu'une « ressource accédante », ou « clé électronique », présente un droit d'accès à une « ressource accédée », ou « serrure électronique », un protocole de vérification du droit d'accès est mis en œuvre. Dans ce mode de réalisation, ce protocole comporte, en plus de la vérification de la plage de validité, la vérification de la signature électronique de cette plage de validité.

Dans ce mode de réalisation, la plage de validité peut être, soit la période proprement dite pendant laquelle il est possible d'accéder à la ressource, soit la période de validité d'une clé de signature de la ressource accédante lui permettant de s'authentifier vis-à-vis de la ressource accédée, soit tout autre paramètre permettant de limiter dans le temps une attaque par utilisation frauduleuse de la ressource accédante.

Comme l'indique la figure 2, dans ce mode de réalisation, une première étape 2001 consiste, de même qu'à l'étape 1001 dans le mode de réalisation précédent, à initialiser la serrure électronique par une valeur de comptage de référence VC_{ref}.

Dans le cas où la signature électronique S utilisée est calculée à l'aide d'un algorithme à clé publique, du type RSA (Rivest Shamir Adleman) par exemple, on mémorise dans la serrure électronique la clé publique K_P de vérification de la signature.

La signature électronique S peut également être calculée à l'aide d'un algorithme à clé secrète, du type DES (Data Encryption Standard) par exemple. Dans ce cas, contrairement au cas précédent, la clé de vérification qui est mémorisée dans la serrure à l'étape 2001 est secrète. De ce fait, elle devra être stockée dans une mémoire physiquement protégée, de sorte qu'elle ne puisse être ni lue, ni modifiée par une entité non autorisée.

On considère ensuite une situation où la clé électronique tente d'accéder à la serrure électronique. De même que dans le mode de réalisation précédent, un protocole de vérification du droit d'accès de cette clé à cette serrure est mis en œuvre successivement dans la clé et dans la serrure.

Dans la clé, comme indiqué en 2002 sur la figure 2, on lit ou on établit une signature électronique S(PH) de la plage horaire prédéterminée PH. Cette étape a lieu, soit en plus, soit en lieu et place de l'étape 1002 de lecture de la plage horaire PH du mode de réalisation précédent.

Cette signature électronique S(PH) peut avoir été calculée au préalable, par exemple par une entité extérieure de calcul de signatures, indépendante de la clé.

Dans ce cas, lors d'une étape de chargement, par exemple au moyen d'une borne de validation, une entité de validation transfère et mémorise la signature S(PH) dans la clé avant que cette clé soit mise en service.

En variante, la clé peut établir elle-même la signature, si on a mémorisé dans la clé électronique la clé privée nécessaire à cette opération, ainsi que l'algorithme cryptographique de signature, et si cette clé dispose des ressources calculatoires nécessaires.

Comme indiqué en 2003, lors de la tentative d'accès, on mémorise dans la clé la valeur horaire courante VH délivrée par l'horloge temps réel de la clé.

Puis on transmet, en 2004, la signature électronique S(PH) de la plage de validité ainsi que la valeur horaire courante VH à la serrure. Si, à l'étape 2002, on a lu la plage horaire PH en plus de la signature S(PH), on transmet également cette plage horaire PH à la serrure à l'étape 2004.

Les étapes suivantes de vérification ont alors lieu dans la serrure.

En 2005, on vérifie la signature transmise. Si l'algorithme de calcul de signatures est un algorithme à clé publique, l'étape 2005 consiste, pour la serrure électronique, à appliquer la clé publique K_P, préalablement

mémorisée dans la serrure, à l'algorithme de vérification. La vérification positive de la signature permet d'assurer l'authenticité de la plage de validité [VH1,VH2], ladite plage étant obtenue, soit par rétablissement du message au cours de l'étape de vérification de signature, soit par simple lecture si elle a été transmise en clair avec la signature.

En 2006 et 2007, on vérifie, d'une part, la cohérence entre la valeur horaire courante transmise VH et la plage horaire prédéterminée PH, et d'autre part, la cohérence entre VH et la valeur de comptage de référence VC_{ref} mémorisée dans la serrure.

Par exemple, dans le cas d'une plage horaire réduite à un intervalle [VH1,VH2], on vérifie que VH est postérieure à VH1 et antérieure à VH2, et que VH est postérieure à VC_{ref}.

Si l'une des vérifications effectuées aux étapes 2005, 2006 et 2007 donne lieu à une réponse négative, on interdit l'accès de cette clé à cette serrure.

Si l'ensemble de ces vérifications a été satisfait, on autorise l'accès, et on met à jour VC_{ref} en la remplaçant par exemple par la valeur horaire courante VH.

Un mode particulier de réalisation du système de contrôle d'accès conforme à la présente invention va maintenant être décrit à l'aide de la figure 3.

Le système comprend une clé électronique 1 et une serrure électronique 2.

La clé électronique 1 comprend un module 11 d'alimentation en énergie, du type pile ou batterie par exemple. Le module 11 alimente une horloge temps réel interne 12 qui délivre une valeur horaire courante VH telle que définie précédemment. La clé 1 comprend également une

mémoire 13, dans laquelle est mémorisée la plage de validité PH.

L'horloge temps réel 12 et la mémoire 13 sont reliées à un module 14 de communication de la clé avec la serrure. Le module 14 permet à la clé, lors de chaque tentative d'accès, de transmettre à un module 21 de communication compris dans la serrure 2 la plage horaire PH mémorisée dans la mémoire 13, ainsi que la valeur horaire courante VH délivrée par l'horloge 12.

Le module 21 de communication de la serrure avec la clé est relié à une mémoire 22 accessible en lecture et en écriture. La mémoire 22 comprend un module 23 de comptage, dans lequel est mémorisée une valeur de comptage de référence VC_{ref}, initialisée avant la mise en service de la serrure électronique et remise à jour à l'aide de la valeur horaire courante VH transmise par la clé 1, à chaque tentative d'accès réussie. La mémoire 22 est par exemple une mémoire reprogrammable électriquement du type EPROM ou EEPROM.

La serrure 2 comprend en outre un module 25 de comparaison, qui reçoit la valeur horaire courante VH transmise par la clé 1, et la compare à la plage horaire prédéfinie PH = [VH1,VH2] et à la valeur de comptage de référence VC_{ref} mémorisée dans le module 23 de comptage. Le module 25 de comparaison teste si $VH > VH1$ et $VH < VH2$, et si $VH > VC_{ref}$.

Le module 11 d'alimentation en énergie de la clé 1 fournit éventuellement à la serrure 2 l'énergie nécessaire aux opérations de vérification effectuées par le module 25 de comparaison, ainsi que l'énergie nécessaire à l'opération de remise à jour du module 23 de comptage en cas de tentative d'accès réussie.

On décrit ci-après, à l'aide de la figure 4, un autre mode de réalisation du système de contrôle d'accès de l'invention, comprenant une clé électronique 41 et une serrure électronique 42, qui procure une sécurité accrue par rapport au mode de réalisation de la figure 3.

Les éléments de ce système qui sont analogues à ceux du mode de réalisation de la figure 3 portent les mêmes chiffres de référence, et ne seront pas décrits une nouvelle fois.

Dans ce mode de réalisation, la mémoire 13 de la clé 41 contient non seulement la plage de validité PH, mais aussi la signature électronique S(PH) de cette plage de validité.

La module 14 de communication de la clé avec la serrure permet à la clé 41, lors de chaque tentative d'accès, de transmettre au module 21 de communication compris dans la serrure 42, non seulement la valeur horaire courante VH délivrée par l'horloge 12 et la plage horaire PH mémorisée dans la mémoire 13, mais aussi la signature électronique S(PH) mémorisée dans la mémoire 13.

La serrure 42 comprend, en plus du module 21 de communication avec la clé, de la mémoire 22 comprenant le module 23 de comptage, et du module 25 de comparaison, décrits précédemment, un module 24 de vérification de signature.

Le module 24 est relié au module 21 de communication de la serrure avec la clé et au module 25 de comparaison. Le module 24 reçoit la signature S(PH) de la plage de validité et, dans le cas où l'algorithme de calcul de signatures utilisé est un algorithme à clé publique, vérifie la signature S(PH) reçue au moyen de la clé publique K_P.

Le module 11 d'alimentation en énergie de la clé 41 fournit éventuellement à la serrure 42 l'énergie nécessaire

aux opérations de vérification effectuées par le module 24 de vérification de signature et le module 25 de comparaison, ainsi que l'énergie nécessaire à l'opération de remise à jour du module 23 de comptage en cas de tentative d'accès réussie.

La figure 5 illustre une réalisation matérielle particulière des modules 14 et 21 de communication entre la clé et la serrure, applicable aussi bien au mode de réalisation de la figure 3 qu'au mode de réalisation de la figure 4.

La clé 1 (ou 41 dans le cas du mode de réalisation de la figure 4) comprend une tige 30 en matière ferromagnétique, garnie d'enroulements en cuivre 31 formant un premier bobinage. Ce premier bobinage est relié au module 14 de communication de la clé avec la serrure.

A chaque tentative d'accès, la clé 1 ou 41 vient se loger dans une cavité tubulaire 32 de diamètre légèrement supérieur au diamètre de la tige 30. La cavité 32 est également garnie d'enroulements en cuivre 33 formant un second bobinage, relié au module 21 de communication de la serrure avec la clé. Les deux bobinages 31, 33 sont alors concentriques, et l'information est transmise sous forme codée binaire entre la clé et la serrure 2 (ou 42 dans le cas du mode de réalisation de la figure 4) par induction électromagnétique.

La présente invention trouve une application particulièrement adaptée à l'accès, par les préposés au courrier, à des boîtes aux lettres, qui ne sont pas autonomes en énergie.

On peut renforcer encore davantage la sécurité du contrôle d'accès, en ajoutant d'autres données aux informations de signature et de plage horaire transmises par

la clé à la serrure. Par exemple, on peut ajouter un numéro de série identifiant la clé électronique. Dans ce cas, on munit la serrure d'un module de comptage supplémentaire, associé à ce numéro de série ; on mémorise dans le module de comptage supplémentaire le début de la prochaine plage horaire au cours de laquelle une clé portant ce numéro de série pourra accéder à la serrure.

REVENDICATIONS

1. Procédé de contrôle d'accès d'au moins une clé électronique, munie d'une horloge temps réel délivrant une valeur horaire courante, à au moins une serrure électronique, à l'intérieur d'une plage horaire prédéterminée, caractérisé en ce que :

(a) on initialise la serrure électronique par une valeur de comptage de référence ;

puis, lors de chaque tentative d'accès de la clé électronique à une serrure électronique :

dans la clé électronique :

(b) on lit une plage horaire prédéterminée, préalablement mémorisée dans la clé électronique ;

(c) on mémorise une valeur horaire courante délivrée par l'horloge temps réel ;

(d) on transmet de la clé électronique à la serrure électronique la plage horaire et la valeur horaire courante, et

dans la serrure électronique :

(e) on vérifie que la valeur horaire courante transmise est à l'intérieur de la plage horaire prédéterminée, et qu'elle est postérieure à la valeur de comptage de référence mémorisée dans la serrure ;

(f) si les vérifications effectuées à l'étape (e) sont satisfaites, on autorise l'accès, et on met à jour la valeur de comptage de référence, à partir de la valeur horaire courante transmise ;

(g) si la valeur horaire courante transmise est à l'extérieur de la plage horaire prédéterminée, ou si elle est antérieure à la valeur de comptage de référence

mémorisée dans la serrure, on interdit l'accès de cette clé à cette serrure.

2. Procédé selon la revendication 1, caractérisé en ce que :

dans la clé électronique :

(b1) à l'étape (b), on lit, en plus de la plage horaire, ou en lieu et place de la plage horaire, une signature électronique de ladite plage horaire, préalablement calculée et mémorisée dans la clé électronique ;

(d1) à l'étape (d), on transmet de la clé électronique à la serrure électronique, en plus de la plage horaire, ou en lieu et place de la plage horaire et de la valeur horaire courante, ladite signature et la valeur horaire courante, et dans la serrure électronique :

(e1) avant l'étape (e), on vérifie la signature transmise, à partir d'une clé de vérification spécifique ;

(f1) à l'étape (f), on n'autorise l'accès, et on ne met à jour la valeur de comptage de référence, à partir de la valeur horaire courante transmise, que si les vérifications effectuées aux étapes (e1) et (e) sont satisfaites ;

(g1) à l'étape (g), on interdit l'accès de ladite clé à ladite serrure si la valeur horaire courante transmise est à l'extérieur de ladite plage horaire, ou si elle est antérieure à la valeur de comptage de référence mémorisée dans la serrure, ou si la vérification effectuée à l'étape (e1) n'est pas satisfaite.

3. Procédé selon la revendication 2, caractérisé en ce que l'ordre d'exécution des étapes (e1) et (e) est interverti.

4. Procédé selon la revendication 2 ou 3, caractérisé en ce que ladite clé de vérification spécifique est une clé publique ou secrète.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ladite plage horaire prédéterminée comprend plusieurs plages horaires disjointes.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce chaque plage horaire est un intervalle comportant deux bornes exprimées chacune comme une date en jour, mois, année et un horaire en heures, minutes, secondes.

7. Système de contrôle d'accès électronique, à l'intérieur d'une plage horaire prédéterminée, comportant au moins une serrure électronique (2;42) et au moins une clé électronique (1;41), caractérisé en ce que
la clé (1;41) comprend

- une horloge temps réel (12) délivrant une valeur horaire courante (VH), et
- des moyens (14) pour transmettre à la serrure (2;42) une plage horaire (PH) prédéterminée, et en ce que

la serrure (2;42) comprend

- des moyens (22) de mémorisation accessibles en lecture et en écriture,
- des moyens (23) de comptage, lesdits moyens (23) de comptage étant mis à jour à partir de ladite valeur horaire courante (VH) à chaque tentative d'accès réussie, et
- des moyens (25) de comparaison de la valeur horaire courante (VH) à la plage horaire (PH) prédéterminée et à la valeur (VC_{ref}) mémorisée dans lesdits moyens (23) de comptage.

8. Système selon la revendication 7, caractérisé en ce que

- lesdits moyens (14) de la clé électronique (1;41) comprennent en outre des moyens pour transmettre à la serrure (2;42) une signature électronique (S(PH)) de ladite plage horaire (PH), et en ce que

- la serrure (2;42) comprend en outre des moyens (24) pour vérifier ladite signature électronique (S(PH)) transmise par la clé (1;41).

9. Système selon la revendication 7 ou 8, caractérisé en ce que lesdits moyens (22) de mémorisation comprennent une mémoire non volatile reprogrammable électriquement.

10. Système selon la revendication 7, 8 ou 9, caractérisé en ce que la clé électronique (1;41) communique avec la serrure électronique (2;42) à l'aide de moyens de transmission sans contact, par induction électromagnétique.

11. Système selon la revendication 10, caractérisé en ce que lesdits moyens de transmission sans contact comprennent un premier bobinage électromagnétique (31) prévu dans la clé (1;41) et un second bobinage électromagnétique (33) prévu dans la serrure (2;42).

12. Système selon la revendication 11, caractérisé en ce que les bobinages (31,33) prévus dans la clé (1;41) et dans la serrure (2;42) sont concentriques.

FIG. 1

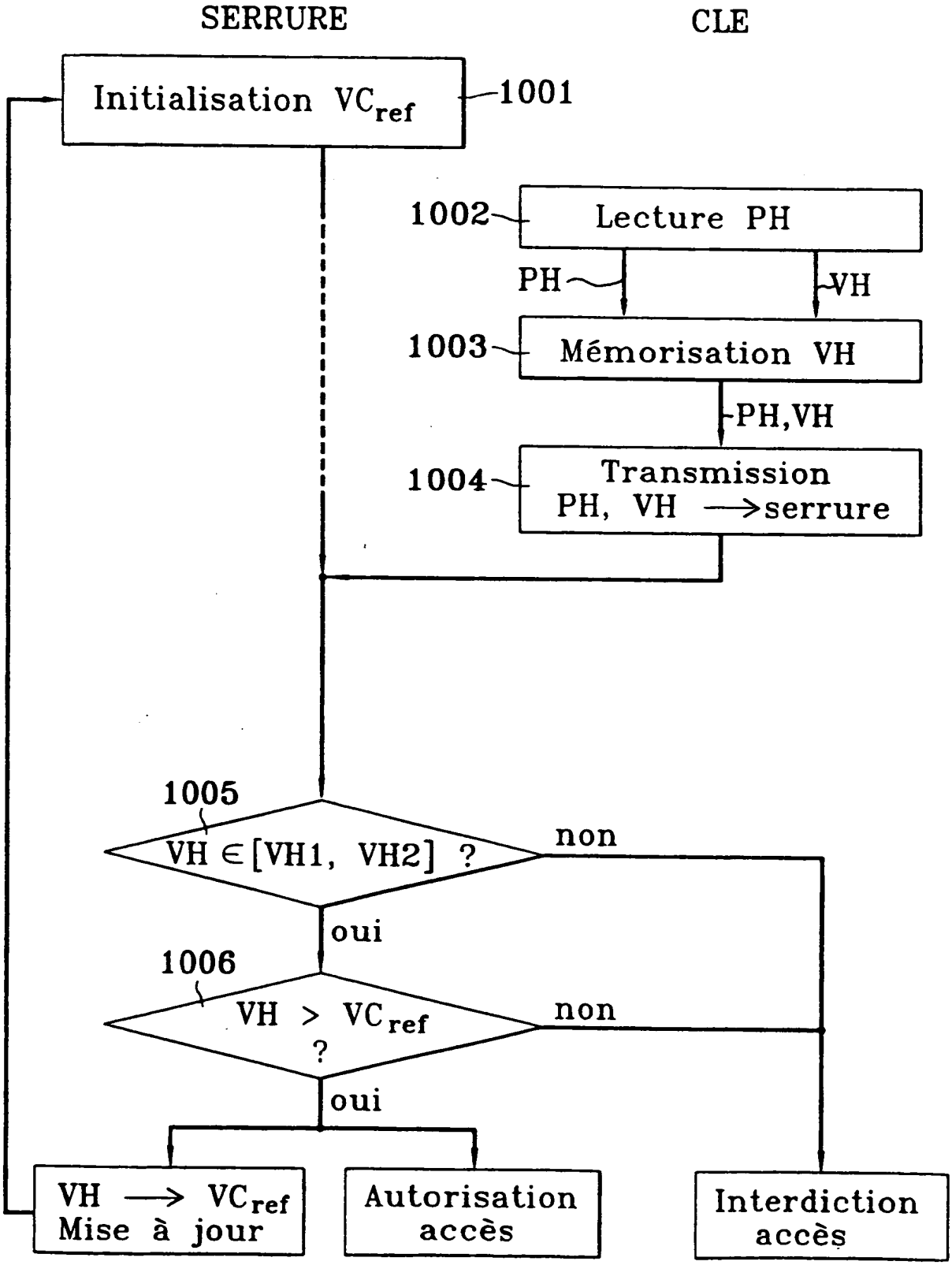

SERRURE
CLE
Initialisation VC_{ref}
1001
1002
Lecture PH
PH
VH
1003
Mémorisation VH
PH,VH
1004
Transmission
PH, VH → serrure
1005
VH ∈ [VH1, VH2] ?
non
oui
1006
VH > VC_{ref} ?
non
oui
VH → VC_{ref}
Mise à jour
Autorisation
accès
Interdiction
accès

FIG.2

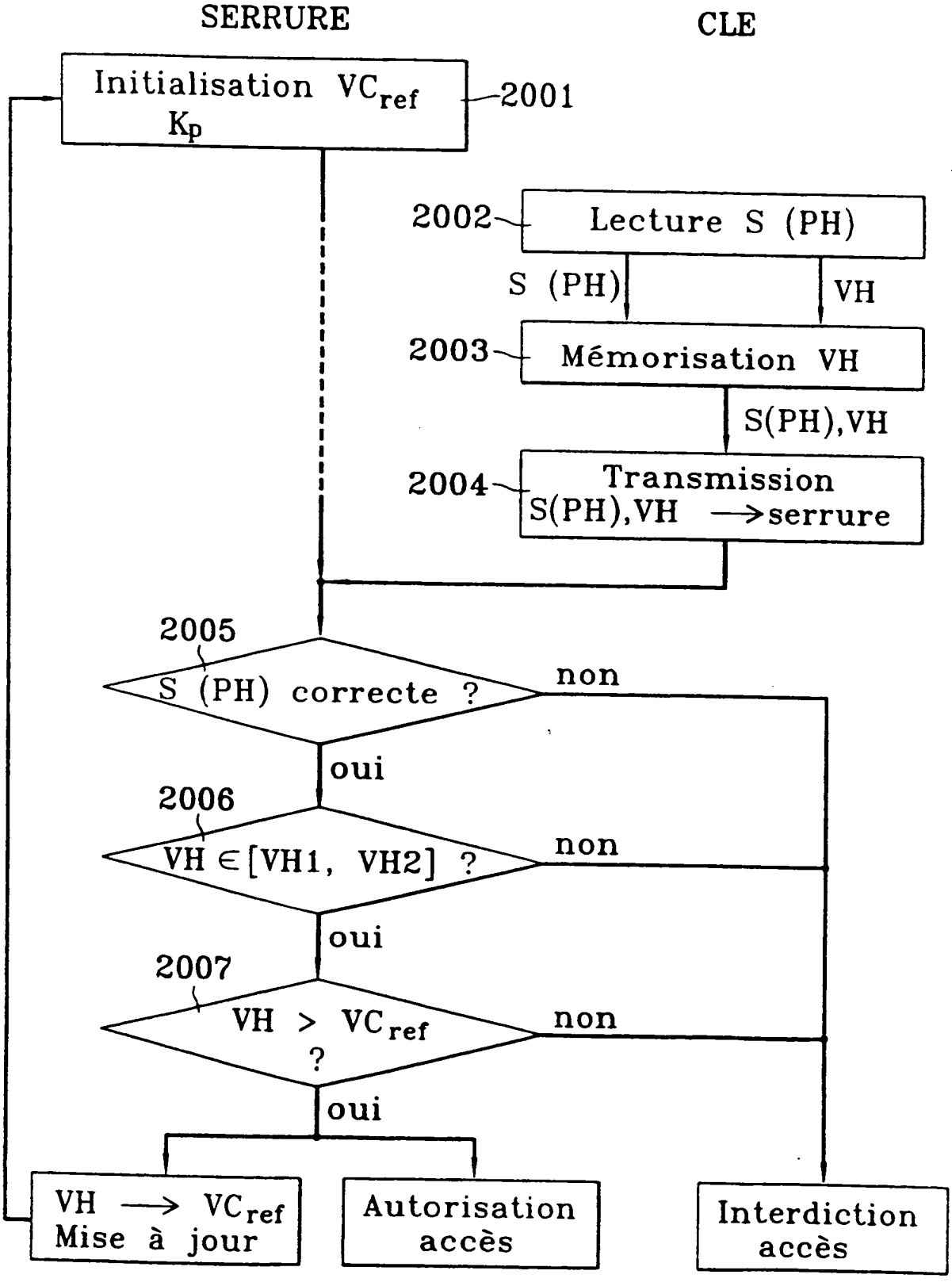

SERRURE
CLE
Initialisation VC_{ref} K_p
2001
2002
Lecture S (PH)
S (PH)
VH
2003
Mémorisation VH
S(PH),VH
2004
Transmission S(PH),VH →serrure
2005
S (PH) correcte ?
non
oui
2006
VH ∈[VH1, VH2] ?
non
oui
2007
VH > VC_{ref} ?
non
oui
VH → VC_{ref} Mise à jour
Autorisation accès
Interdiction accès

FIG.3

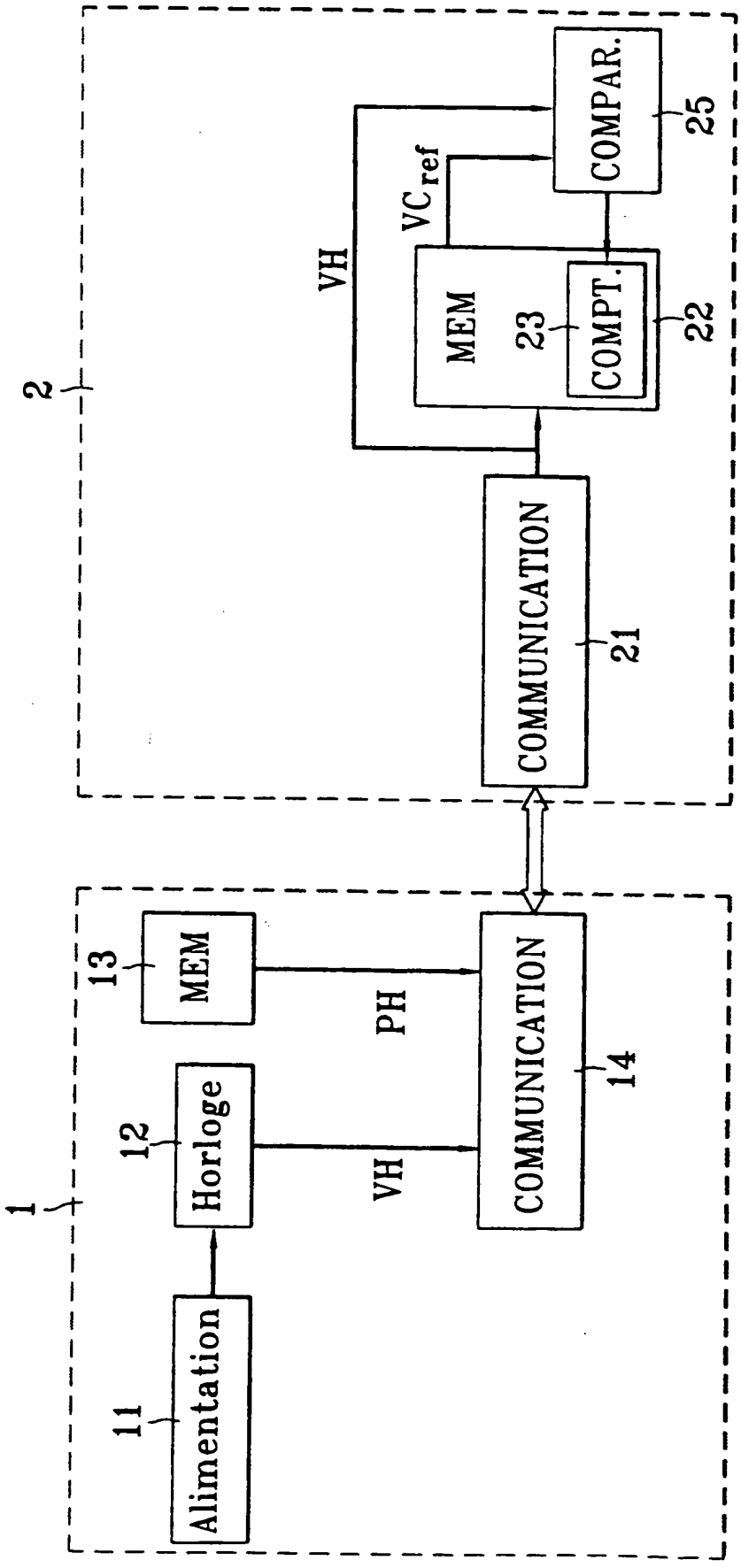

1
2
11
Alimentation
12
Horloge
13
MEM
VH
PH
COMMUNICATION
14
COMMUNICATION
21
VH
MEM
23
COMPT.
22
VC_{ref}
COMPAR.
25

FIG. 4

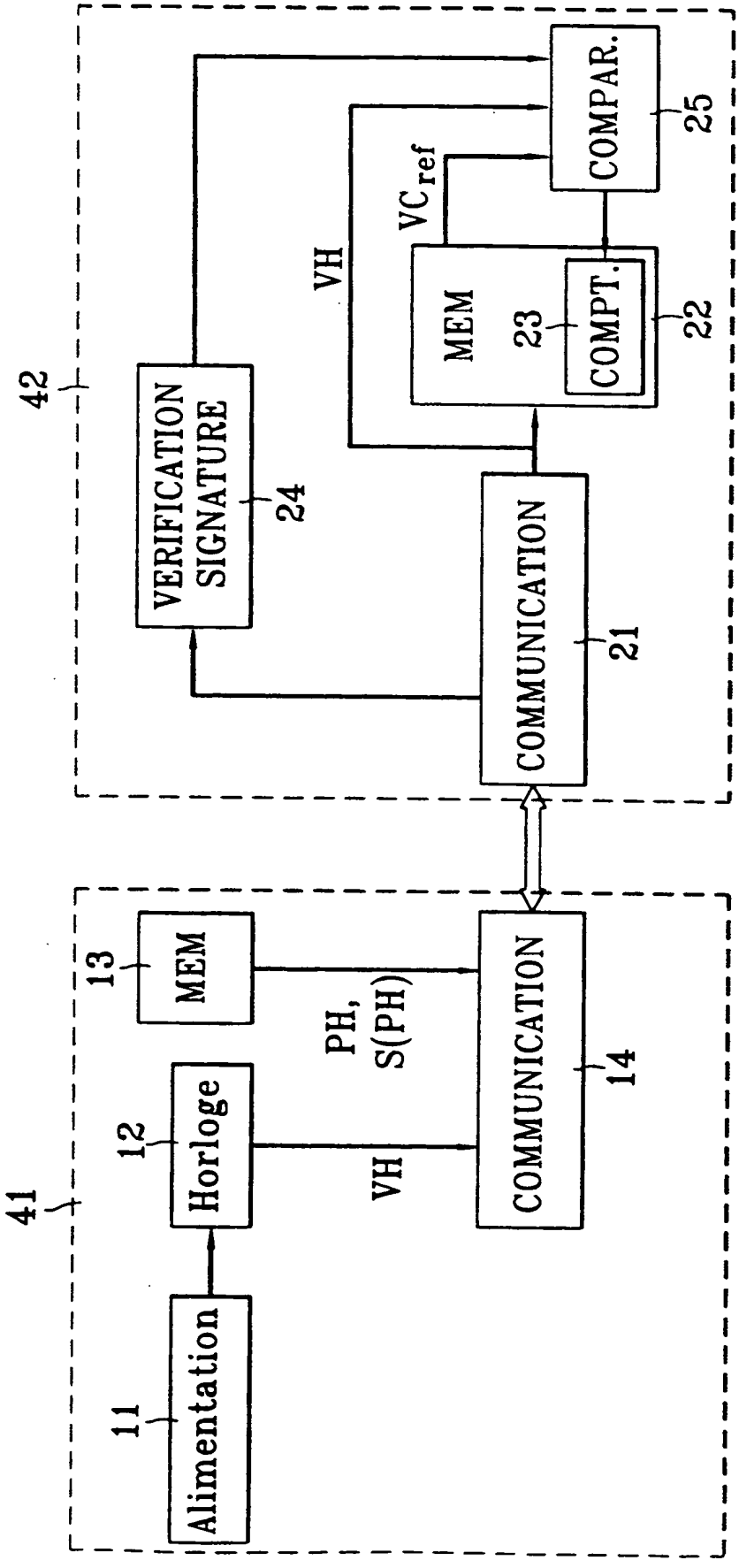
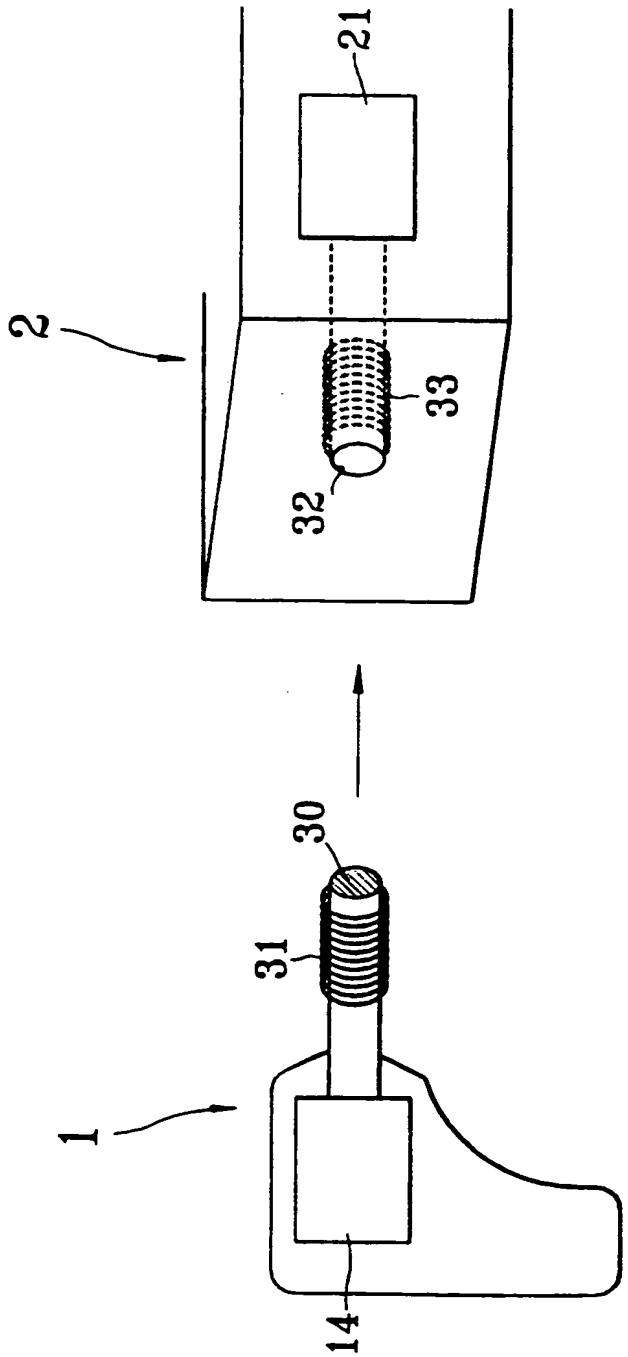

41
42
Alimentation
11
Horloge
12
MEM
13
COMMUNICATION
14
PH,
S(PH)
VH
COMMUNICATION
21
VERIFICATION
SIGNATURE
24
MEM
23
COMPT.
22
VH
VC ref
COMPAR.
25

FIG.5



INTERNATIONAL SEARCH REPORT

Inter .nal Application No
PCT/FR 99/00023

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07C E05B G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 93 21712 A (MEDECO SECURITY LOCKS) 28 October 1993 see abstract; figures 1A,5,6,8,10 see page 2, line 21 - page 3, line 32 see page 5, line 12 - line 31 see page 7, line 18 - page 8, line 8 see page 9, line 1 - line 30 see page 11, line 11 - page 12, line 3 see page 17, line 32 - page 18, line 9 ---	1,7,9
Y	EP 0 419 306 A (ROCKWELL AUTOMOTIVE BODY SYST) 27 March 1991 see abstract; claims 3,4 see page 5, line 14 - line 20 --- -/--	1,7,9

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 April 1999	20/04/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 99/00023

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 722 596 A (FRANCE TELECOM) 19 January 1996 cited in the application see abstract; claims 1-3,9,14; figures see page 3, line 6 - page 5, line 9 see page 6, line 22 - page 7, line 31 see page 11, line 20 - page 12, line 3	1,2,4-8
A	EP 0 122 244 A (WSO CPU SYSTEM AB) 17 October 1984 see abstract; figures	1,7,9
A	WO 82 02811 A (NELSON AVI N) 19 August 1982 see abstract; figure 1 see page 1, line 13 - page 2, line 34	10-12

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ...nal Application No
PCT/FR 99/00023

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9321712 A	28-10-1993	US 5745044 A	28-04-1998
		CA 2133743 A,C	28-10-1993
		EP 0635182 A	25-01-1995
		JP 7505988 T	29-06-1995
		US 5541581 A	30-07-1996
EP 0419306 A	27-03-1991	FR 2652216 A	22-03-1991
		CA 2025312 A,C	21-03-1991
		DE 69017335 D	06-04-1995
		DE 69017335 T	06-07-1995
		JP 3206748 A	10-09-1991
		US 5101430 A	31-03-1992
FR 2722596 A	19-01-1996	AT 175796 T	15-01-1999
		AU 2931795 A	16-02-1996
		CA 2171626 A	01-02-1996
		DE 69507278 D	25-02-1999
		EP 0719438 A	03-07-1996
		WO 9602899 A	01-02-1996
		JP 9503089 T	25-03-1997
		US 5768379 A	16-06-1998
EP 0122244 A	17-10-1984	AT 34796 T	15-06-1988
		CA 1217546 A	03-02-1987
		DE 3471712 A	07-07-1988
		JP 59199972 A	13-11-1984
WO 8202811 A	19-08-1982	EP 0071600 A	16-02-1983
		JP 58500203 A	10-02-1983

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dema... Internationale No
PCT/FR 99/00023

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 9321712	A	28-10-1993	US	5745044 A	28-04-1998
			CA	2133743 A,C	28-10-1993
			EP	0635182 A	25-01-1995
			JP	7505988 T	29-06-1995
			US	5541581 A	30-07-1996
EP 0419306	A	27-03-1991	FR	2652216 A	22-03-1991
			CA	2025312 A,C	21-03-1991
			DE	69017335 D	06-04-1995
			DE	69017335 T	06-07-1995
			JP	3206748 A	10-09-1991
			US	5101430 A	31-03-1992
FR 2722596	A	19-01-1996	AT	175796 T	15-01-1999
			AU	2931795 A	16-02-1996
			CA	2171626 A	01-02-1996
			DE	69507278 D	25-02-1999
			EP	0719438 A	03-07-1996
			WO	9602899 A	01-02-1996
			JP	9503089 T	25-03-1997
			US	5768379 A	16-06-1998
EP 0122244	A	17-10-1984	AT	34796 T	15-06-1988
			CA	1217546 A	03-02-1987
			DE	3471712 A	07-07-1988
			JP	59199972 A	13-11-1984
WO 8202811	A	19-08-1982	EP	0071600 A	16-02-1983
			JP	58500203 A	10-02-1983

RAPPORT DE RECHERCHE INTERNATIONALE

Dem. Internationale No
PCT/FR 99/00023

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	FR 2 722 596 A (FRANCE TELECOM) 19 janvier 1996 cité dans la demande voir abrégé; revendications 1-3,9,14; figures voir page 3, ligne 6 - page 5, ligne 9 voir page 6, ligne 22 - page 7, ligne 31 voir page 11, ligne 20 - page 12, ligne 3	1,2,4-8
A	EP 0 122 244 A (WSO CPU SYSTEM AB) 17 octobre 1984 voir abrégé; figures	1,7,9
A	WO 82 02811 A (NELSON AVI N) 19 août 1982 voir abrégé; figure 1 voir page 1, ligne 13 - page 2, ligne 34	10-12

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 99/00023

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07C9/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07C E05B G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	WO 93 21712 A (MEDECO SECURITY LOCKS) 28 octobre 1993 voir abrégé; figures 1A,5,6,8,10 voir page 2, ligne 21 - page 3, ligne 32 voir page 5, ligne 12 - ligne 31 voir page 7, ligne 18 - page 8, ligne 8 voir page 9, ligne 1 - ligne 30 voir page 11, ligne 11 - page 12, ligne 3 voir page 17, ligne 32 - page 18, ligne 9	1,7,9
Y	EP 0 419 306 A (ROCKWELL AUTOMOTIVE BODY SYST) 27 mars 1991 voir abrégé; revendications 3,4 voir page 5, ligne 14 - ligne 20	1,7,9

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégones spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
6 avril 1999	20/04/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Europeen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)